



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/598,777	06/16/2000	Steven H. McCown	00-022-MIS	5604

7590 04/14/2003

Wayne P Bailey  
Storage Technology Corporation  
One StorageTek Drive  
Louisville, CO 80028-4309

EXAMINER

LE, DAVID Q

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 04/14/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/598,777

Applicant(s)

MCCOWN ET AL.

Examiner

David Q Le

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

Art Unit: 3621

## DETAILED ACTION

### *Examiner's Note*

1. The Examiner has pointed out particular references contained in the prior art of record in the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures apply as well. It is requested from the Applicant, in preparing the response, to consider fully the entire references as well as the context of all passages in the cited references as potentially teaching all or part of the claimed inventions.

### *Status of Claims*

2. Claims 1, 8, 11, 13, 19-20, 22-24, 32, 39-40 were amended as requested in the Amendment filed on January 23 2003.

Claims 1-40 remain pending.

### *Response to Amendment & Request for Consideration*

3. Applicant's arguments with respect to the original claims 1-40 have been considered but are moot in view of the new ground(s) of rejection as applied to the amended claims 1-40.

### *Claim Rejections - 35 USC § 102*

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 3621

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-2, 5, 7-8, 11-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Muftic, US Patent 5,850,442.

As per claim 1.

Muftic discloses

A method for securing a transaction in order to prevent fraudulent transactions (Abstract, Summary of the Invention), said method comprising:

receiving, prior to the transaction, a secret master key (Fig 16: "smart token/certificate", associated text) from a third party, wherein the master key remains unchanged and is kept secret and is not altered after the transaction, the third party storing a copy of the master key (Fig 16, associated text);

receiving a request for a digest (C2, L27-51: "message digest") from a requestor (Fig 10: step 1030: "receive order form"; associated text);

retrieving the master key (Fig 10: step 1060: "digitally sign order form");

retrieving unique client information (Fig 10, steps 1040, 1060);

the client information being associated with the master key (Fig 10 : step 1060);

creating the digest by hashing the unique client information and the master key (C2, L38-41);

and

returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with a third party (Fig 10: step 1060).

As per claim 8.

Muftic discloses

A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

initializing a smart card (C4, L33-43; Fig 3, associated text) by receiving within the card a secret master key from a credit card issuer, the master key being kept secret (Fig 16: "smart token/certificate", associated text);

Art Unit: 3621

receiving, into the smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information (Fig 16: "seller's ID"), and a request for a billing digest (C2, L15-51: "message digest"; Fig 10: step 1030: "receive order form"; associated text);

retrieving unique client information, from the smart card memory (Fig 10, steps 1040, 1060);  
retrieving the master key, the master key being known to the credit card issuer (Fig 10: step 1060);

creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card (C2, L38-41 and

passing the billing digest, the unique merchant information and the unique client information to the requestor (Fig 10: step 1060).

**As per claim 11.**

Muftic discloses

A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

initializing a smart card (C4, L33-43; Fig 3, associated text) by receiving within the card a secret master key from a credit card issuer, the master key being kept secret (Fig 16: "smart token/certificate", associated text);

sending a data transmission to the client's smart card, wherein the data transmission includes unique merchant information and a request for a billing digest (C2, L15-51: "message digest"; Fig 10: step 1030: "receive order form"; Fig 16: "seller's ID", associated text);

receiving the billing digest, the unique merchant information and unique client information from the smart card, the billing digest being hashed from the unique merchant information, unique client information and the master key from the smart card (Fig 10: step 1060); and

transmitting the unique merchant information and unique client information from the smart card to a credit card issuer (Fig 13, associated text).

**As per claim 2.**

Muftic discloses all the limitations of claim 1.

Muftic further discloses

the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information (Fig 16: "seller's ID").

Art Unit: 3621

As per **claim 5**

Muftic discloses all the limitations of claim 1.

Muftic further discloses

creating the digest by hashing is performed by a smart card (C4, L33-43; Fig 3, associated text).

As per **claim 7**.

Muftic discloses all the limitations of claim 1.

Muftic further discloses

the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client (Fig 13, associated text).

As per **claim 12**.

Muftic discloses all the limitations of claim 11.

Muftic further discloses

receiving a response from the credit card issuer (Fig 13, associated text).

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 3, 6, 9-10, 14, 17-26, 28-33, 36-38** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Muftic**, US Patent 5,850,442.

Art Unit: 3621

As per claim 13.

Muftic discloses

A method for securing a transaction comprising:

receiving a transaction request from a requestor, wherein the request includes a digest and unique client information (see above citations, from claims 1, 8, 11).

Muftic does not explicitly recite all the steps of:

accessing a master key based on the unique client information;

creating an authorization digest by hashing the unique client information and the master key;

comparing the authorization digest with the digest from the requestor; and

returning a response to the requestor, the content

of the response being based on an outcome of the comparison of the authorization digest with the digest from the requestor.

However Muftic does disclose providing a token or certificate (i.e. "master key") assigned to a unique client account (see citations used in claims 1, 8, 11) and the authorization process performed at a credit card issuer or bank (Fig 13, associated text) using well-known methods for authenticating a client, merchant, and transaction to be authorized.

Muftic also discloses that when using hashes, the method for determining if a message is authentic is by doing a similar hash and comparing the results (C2, L27-37). Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made that in order to perform a proper validation and authorization of a transaction, the authorizing entity must inherently perform a parallel hashing of merchant, client, transaction IDs, and matching master key, and then compare the resulting digest with the one received from a requestor, in order to determine whether the request may be authorized.

As per claims 20-24, 32, 39, 40.

Muftic discloses all the limitations of these claims (see all above citations) except for the specific steps of hashing the same components of a message digest and comparing the resulting digest with an authorization request in order to determine whether to authorize that request.

Art Unit: 3621

However, as analyzed above in claim 13, Muftic clearly teaches that the way to authenticate a hashed message is by using the same components, doing a parallel hash, and comparing the results.

Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made to include these steps in the authentication of authorization requests, so that proper validation and authentication may be done. The resulting systems would have met all the limitations of claims 20-24, 32, 39, 40.

As per claims 3, 14, 25, 26, 33.

Muftic discloses all the limitations of claims 1, 13, 24, 32.

Muftic does not specifically recite that

the request includes unique merchant information which is used to access the master key.

However Muftic teaches that merchants also need to have specific accounts with credit card issuers in order to obtain credit for the transactions they enter into with clients (Fig 16: steps 1610, 1620). It is also well-known in the art that all merchants wishing to participate in a electronic commerce system need to establish accounts in advance with banks, credit card issues, clearing houses, and the like. Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made to ensure that a request for billing digest would include unique merchant information that would dictate which master key the client system will fetch (i.e. Visa, Mastercard, AMEX, etc.). This would be inherent in the system, in order to allow it to properly match account holders and financial institutions.

As per claims 17, 28, 36.

Muftic discloses all the limitations of claims 13, 24, 32.

Muftic further discloses

creating the digest by hashing is performed by a smart card (C4, L33-43; Fig 3, associated text).

As per claims 6, 10, 18, 29, 37.

Muftic discloses all the limitations of claims 1, 8, 13, 24, 32.

Muftic further discloses that encryption will be used in his system (C7, L1-15).

Muftic does not specifically recite

Encrypting/decrypting the unique client information.



Art Unit: 3621

However it would be obvious to one ordinarily skilled in the art at the time the invention was made that all unique client information (i.e. certificates, signatures) would need to be kept secure to prevent unauthorized access or capture. Therefore it would just be common sense to encrypt this client information before retrieving it and transmitting it to a vendor.

As per claims 19, 30, 38.

Muftic discloses all the limitations of claims 13, 24, 32.

Muftic further discloses

the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client (Fig 13, associated text).

As per claim 31.

Muftic discloses all the limitations of claim 24.

Muftic further discloses using a biometric for enhanced security of his system (C16, L41-51).

8. Claims 4, 9, 15-16, 27, 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic and further in view of Nguyen et al., US Patent 5,931,917.

Muftic discloses all the limitations of claims 1, 8, 13, 24, 32.

Muftic does not disclose using reference numbers and checking to see if old reference numbers have already been used when authorizing requests for transaction authorizations.

Nguyen discloses

the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party (C26, L19; C28, L17; C29, L57; C37, L25).

It would have been obvious to one ordinarily skilled in the art at the time the invention was made to add reference numbers to the client information as taught by Nguyen, in order to further be

Art Unit: 3621

able to prevent fraudulent transactions: each transaction authorized by the issuer may be assigned a new reference number, thereby preventing the authorization of multiple requests for the same transaction.

**Conclusion**

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Q Le whose telephone number is 703-305-4567. The examiner can normally be reached on 8:30am-5:30pm Mo-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P Trammell can be reached on 703-305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-8494 for regular communications and 703-746-8494 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

DQL

April 7, 2003

  
JAMES P. TRAMMELL  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3600